Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 22 April 2004

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports government inspectors have identified serious weaknesses in security at university laboratories that perform research on anthrax and other dangerous substances. (See item 18)

- The US−CERT has released "Technical Cyber Security Alert TA04−111B: Cisco IOS SNMP Message Handling Vulnerability." (See item 23)

- eSecurity Planet reports a week after Microsoft announced a SSL vulnerability affecting key Windows products, malicious hackers unveiled exploits that could lead to widespread denial−of−service attacks. (See item 26)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *April 21, Reuters* — **U.S. gasoline supplies up as refiners boost rates.** U.S. gasoline supplies rose last week as the nation's refiners made use of glittering profit margins to buff up stocks ahead of the summer driving season, the government said Wednesday, April 21. Gasoline supplies increased by 1.6 million barrels while refinery run rates rose 557,000 barrels per day, according to the Energy Information Administration's (EIA) weekly report. The increase in refining activity triggered a smaller−than−expected crude oil supply build of 200,000 barrels,

the report showed. **The increases in supply were not enough to pull stocks out of a deficit, with crude oil stocks 19.3 million barrels below the five−year average, and gasoline stocks 8.5 million barrels below the five−year average, the EIA said.** The gains in gasoline supply came as U.S. total gasoline imports hit a record of 1.3 million barrels per day, mingling with the higher domestic production rates, the EIA said. **High prices for gasoline, now running at record rates at the pumps, have boosted refiner profit margins and widened the economic window for trans−Atlantic shipments.**
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2004_04_21_eng−reuters_pma_US−GASOLINE−SUPPLIES−UP−AS−REFINERS−BOOST−RATES−EIA&SMContentSet=0

2. *April 21, Rocky Mountain News (CO)* — **Shortage of sand disturbs gas producers. The Rocky Mountains are saturated with natural gas, but the problem is bringing it to the surface. There aren't enough steel pipes or even fine sands needed to extract the gas that is trapped between layers of hard rock. Local gas producers say the shortage of materials could slow down drilling and fracing in the Rockies −− and ultimately affect gas production.** Fracing is the pumping of material into wells to increase gas production. "I would be surprised if everyone hit their (production) targets," said David Kornder, chief financial officer of Patina Oil & Gas Corp. "It is going to be difficult, given the shortage in materials." Companies use sand to prop open the fractures they make in layers of rock to improve the flow of natural gas into underground pipes. The sand is usually imported on freight cars from neighboring states such as Kansas, Texas and Utah. However, supply has tightened in recent months, as demand from gas producers has skyrocketed. Moreover, surging steel prices in the U.S. have increased the cost of steel products such as pipes and tubes used in gas drilling.
Source: http://www.rockymountainnews.com/drmn/business/article/0,1299,DRMN_4_2824211,00.html

[Return to top]

Chemical Sector

3. *April 21, TheIowaChannel.com* — **Ammonia tank leaks in farm field. Authorities say about 50 pounds of a dangerous chemical was accidentally released from a tank parked in a farm field near Huxley in central Iowa.** Mike Dougherty, of Huxley, noticed the ammonia leak near 282nd Street and Highway 69 Tuesday night and called authorities. The Huxley Fire Department stopped the leak and Dougherty was given instructions on how to seal off his home. Two other homes were voluntarily evacuated. Doughery said his family stayed indoors for a few hours and waited for the air to clear. Some residents complained about minor eye irritation, but no one was taken to the hospital.
Source: http://www.theiowachannel.com/news/3026989/detail.html

4. *April 21, The Australian* — **Two killed in Chinese chemical blast. Two female workers were killed and another injured today, April 21, in a chemical blast at a workshop in east China's Taizhou city, Zhejiang province, China's state media reported.** The explosion follows last Thursday's deadly chlorine leak from the Tianyuan Chemical Industry Plant in Chongqing, south−west China, that left nine dead or missing and forced the evacuation of 150,000 people. **Today's explosion was at a Haizheng pharmaceutical group workshop just**

after midnight, Xinhua news agency said, adding the three workers were from the next workshop. Quoting a local fire brigade source, the agency said the blast was caused by the leaking of liquid ammonia and toluene, although it said the cause of the accident was still under investigation.
Source: http://www.theaustralian.news.com.au/common/story_page/0,574 4,9353049^1702,00.html

[Return to top]

Defense Industrial Base Sector

5. *April 21, Government Computer News* — **Defense plans to replace command and control system. The Department of Defense's (DoD) Global Command and Control System (GCCS) is getting unwieldy and will be replaced beginning in 2006**, Defense Information Systems Agency (DISA) officials said Tuesday, April 20. **In place of GCCS will be a new set of applications known as JC2, or Joint Command and Control. JC2 will use Web services and fit with DoD's plan for netcentric warfare,** said Dawn C. Meyerriecks, DISA's chief technology officer. Meyerriecks said GCCS is insufficiently scalable, runs obsolete versions of Sun Microsystems Inc.'s Solaris operating system and Oracle Corp.'s database, and is the wrong architecture. Bernal Allen, chief of DISA's Enterprise Application Division, said one more full version of GCCS, Version 4, will come out in the second quarter of 2006; the first block of JC2 will arrive in the fourth quarter of that year. The technology path DISA and the armed services are on now is to separate the data transport infrastructure, the OS and Web services, applications and data, so that each can be updated independently. Also, GCCS, with its client−server architecture, can't be extended to individual warfighters the way officials envision JC2 being able to, Meyerriecks said.
Source: http://www.gcn.com/vol1_no1/daily−updates/25644−1.html

[Return to top]

Banking and Finance Sector

6. *April 21, Sydney Morning Herald (Australia)* — **Scammers target ANZ and CBA with new tactic.** Scammers are targeting two of Australia's big banks this morning, April 21, with e−mails that have a new twist. **Scam e−mails, apparently from Commonwealth Bank and the ANZ, inform customers that the bank's regular online banking site is unable to handle their online banking due to a denial of service. Hence, the e−mails say, customers should visit another site −− which includes the words "antiddos" in the URL.** According to Daniel McNamara, a systems administrator from Canberra who tracks these scams, the idea is to lure users to a site where a trojan can be loaded onto the user's PC. This trojan logs keystrokes whenever an online banking site is accessed on the PC in question and these keystrokes are sent to an e−mail address specified within the trojan's code. "The domain being used appears down at the moment but we think it may be moved to another server during the day," McNamara said.
Source: http://www.smh.com.au/articles/2004/04/21/1082395898412.html

7.

April 20, KLAS−TV (NV) — **DMV identity theft team. A popular place for identity theft has been at Department of Motor Vehicles (DMV) offices, however, that is changing. The Nevada Department of Motor Vehicles has established its own enforcement unit to stop the crime.** The document fraud unit has been in place for six months now. It consists of four investigators and a document examiner. Since October, the group has made 25 arrests, while opening 400 cases. DMV investigator Thomas Newsome explained that they "look for name, social security number and date of birth matches. Because there are many different scenarios in which someone else's information can be used. For instance, someone may use a child's information, a grandmother, a deceased person's information." **The new digital driver's license also allows technicians to catch identity theft as well.** The Nevada Homeland Security Bill made it a felony for anyone in possession of fraudulent identity documents.
Source: http://www.klas−tv.com/Global/story.asp?S=1801347&nav=168XMS ZJ

[Return to top]

Transportation Sector

8. *April 21, Associated Press* — **Security mix−up clears concourses at Bradley. Two travelers dressed almost identically caused a mix−up in Connecticut’s Bradley International Airport screening area Tuesday, April 20, leading officials to clear two concourses and make everyone pass through security again,** the Transportation Security Administration (TSA) said. The first traveler was leaving the screening area just as the second traveler was entering, confusing a security official. "When he saw the one gentleman leave the area dressed like the other guy, he thought he had left the area without being screened," TSA spokesperson Ann Davis said. Because of the mix−up, officials closed the security area while they reviewed the surveillance video. During that time, all the passengers who had passed through security were ordered out of two airport concourses for re−screening. That included passengers who had just boarded planes, Davis said. The confusion ended after officials reviewed the video and determined that nobody had breached airport security. The review created a 49−minute holdup in the airport, but Davis said no flights were canceled.
Source: http://www.newsday.com/news/local/wire/ny−bc−ct−brf−−airport confus0420apr20,0,4951104.story?coll=ny−ap−regional−wire

9. *April 21, CNN* — **New Jersey fuel tanker accident halts commuters.** A fuel tanker flipped over while making a turn onto a heavily traveled roadway early Wednesday, April 21, in northern New Jersey, authorities said. **The tanker was carrying around 5,000 gallons of diesel fuel when it flipped over while the driver was making a turn from Route 3 onto Route 46 West in Clifton, near Passaic, Clifton police said.** Authorities shut down the east− and westbound lanes of Route 46 and parts of Route 3. "It was a straight tanker truck that flipped over on its side and spilled a couple thousand gallons of diesel fuel. We have tankers on the scene offloading fuel that is still on the tanker," Lt. Paul Tomanek said. The offices of Emergency Management and Environmental Protection were on site overseeing the cleanup, which will take a couple of hours, said Capt. Kenneth Snagusky, coordinator for municipal Office of Emergency Management. "They are attempting to reopen the eastbound lane soon," Snagusky said. The driver was taken to an area hospital with minor injuries, authorities said.
Source: http://www.cnn.com/2004/US/Northeast/04/21/tanker.accident/i ndex.html

10. *April 21, Department of Transportation* — **Department of Transportation Secretary Mineta announces second round of flight reductions at O’Hare.** Department of Transportation Secretary Norman Y. Mineta today, April 21, announced new reductions in United and American Airlines flight schedules aimed at further reducing congestion and passenger inconvenience at Chicago’s O'Hare International Airport. **Speaking to reporters in a telephone news conference, Secretary Mineta revealed plans by United and American Airlines to reduce their daily schedules by another 2.5 percent starting in early June, the second time the airlines have had to trim schedules to help reduce congestion at O’Hare.** Both airlines will reschedule the majority of targeted flights to slower times of the day, but each also has plans to cancel a handful of operations, Secretary Mineta said. A total of 17 United and 12 American flights are affected by the announcement. “No matter how you look at it, these are tough decisions for the airlines,” Secretary Mineta said. “But the consequences of doing nothing would be worse and far−reaching,” he said, noting delays at O’Hare can impact “as many as 40 airports and thousands of travelers nationwide in a matter of minutes.”
Source: http://www.dot.gov/affairs/dot5304.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

11. *April 21, Associated Press* — **Mad cow cases in Japan are in dispute.** Two cases in Japan are at the center of a disagreement between the U.S. and Japan on the risk of mad cow disease in young cows. **American consumers have been assured that cattle under 30 months of age are unlikely to contract the disease. That assurance is the underpinning of the U.S. Department of Agriculture's (USDA) trade policies and its expanded mad cow surveillance program to test high−risk cattle.** The government's stricter slaughterhouse regulations also cite 30 months as the cutoff age for special handling of meat. **But Japanese officials say they have found two mad cow cases in their country involving animals under the age of 30 months.** Sato Tadashi, Japanese agriculture attache said that Japan is "seriously concerned" about the United States' insistence that cattle under 30 months of age are not at risk for mad cow disease. **Ron DeHaven, administrator of the USDA's Animal and Plant Health Inspection Service, said that those two animals tested positive on two of the three types of tests but showed negative on the more precise immunohistochemistry test.** DeHaven said there is no international consensus about whether the two young Japanese animals were positive for mad cow disease. "We need to put it in the context of two animals out of tens of thousands, I think internationally 185,000 plus or minus positive animals," he said.
Source: http://www.kansas.com/mld/eagle/business/8480698.htm

12. *April 21, Globe and Mail (Canada)* — **Avian flu contained in Canada. With only two new flocks testing positive for avian flu in the past six days, the Canadian Food Inspection Agency says the spread of the deadly virus may have finally been contained.** "We appear to

be getting ahead of this disease," said Cornelius Kiley, a veterinarian with the agency. About 950,000 infected birds in the Fraser Valley have now been destroyed on 26 of 31 farms where the H7N3 avian flu virus was detected. About 175,000 birds have yet to be killed on five remaining farms.
Source: http://www.theglobeandmail.com/servlet/ArticleNews/TPStory/LAC/20040421/NATS21−4/TPNational/Briefs

13. *April 20, Animal and Plant Health Inspection Service* — **France and Spain free of classical swine fever. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is amending its regulations to recognize France and Spain as regions free of classical swine fever (CSF).** Eradicated from the United States in 1978, swine fever is a highly contagious viral disease affecting swine. This action adds France and Spain to the regions within the European Union that were recognized in April 2003 as regions free of CSF. APHIS now recognizes the following countries as CSF free: Austria, Belgium, France, Greece, the Netherlands, Portugal, Spain, and most of Germany and Italy. **Breeding swine, swine semen, and pork and pork products can be imported under certain conditions from CSF free regions only if they have not been commingled with animals and animal products where the disease occurs.** These animals and products are still subject to additional restrictions if other foreign swine diseases of concern to the United States are present. This final rule is published in the April 20 Federal Register and becomes effective April 20.
Source: http://www.aphis.usda.gov/lpa/news/2004/04/csffree_vs.html

[Return to top]

Food Sector

14. *April 21, Food Production Daily* — **Action behind foodborne disease. Comprehension of how Listeria monocytogenes invades mammalian cells during infection is vital to understanding how this foodborne disease can change from inducing gastroenteritis to serious complications like meningitis, septicaemia, abortion, and even death.** Scientists from the Institut Pasteur in Paris describe how two mammalian proteins, myosin VIIa and vezatin, are hijacked by Listreia and used in the propagation of the infection within the host. **It is the bacteria’s capacity to cross, initially the intestinal wall and later the brain barrier and/or the placenta, three body barriers normally capable of withholding the invasion of infectious agents, that allows the spread of listeriosis and makes it such a big threat to the host.** The researchers describe how disruption in the function of any of these two host proteins leads to an immediate reduction in the number of infected cells, indicating that myosin VIIa and vezatin are crucial for Listeria’s cell invasion. The team of scientists also report that both these proteins are recruited to the site of the bacteria’s entrance during its internalization. Researchers propose that the mechanism of Listeria internalization depends on highjacking the host’s myosin VIIa and vezatin and using them to create the force that “pushes” the bacteria into the cells.
Source: http://www.foodproductiondaily.com/news/news−NG.asp?id=51526

[Return to top]

Water Sector

15. *April 21, Shawnee News−Star (Oklahoma)* — **Low lake levels prompt water rationing.** Shawnee, OK officials abruptly enacted mandatory Level Three water rationing, which became effective Wednesday, April 21. "We're going to be in serious trouble if we don't do something, if we don't get some rain," said Acting City Manager Terry Compton. Public Works Director James Cole said lake levels at Shawnee Twin Lakes are between 1,066 and 1,067 above sea level. "That's lower than they were at any point last summer," Cole said. **Shawnee enacted voluntary Level One rationing last summer, but never had to go to mandatory.** On Level Three, odd−numbered residences, for other than household purposes, can water from 12:01 a.m. to 1 p.m. on Tuesdays only. Even−numbered residences can water from 12:01 a.m. to 1 p.m. on Thursdays only. Exterior commercial use is restricted to the same days and hours. The city's water rationing policy shows Level Three rationing occurs when the lake level reaches an elevation of 1,068 feet and the average daily usuage exceeds 5 million gallons for seven days. "The trouble is we are nearly the end of April and we haven't had any appreciable rain and we had two days last week that we had over 4 million gallons usage," Compton said.
Source: http://www.news−star.com/stories/042004/New_34.shtml

16. *March 19, General Accounting Office* — **GAO−04−461: Comprehensive Asset Management Has Potential to Help Utilities Better Indentify Needs and Plan Future Investments (Report).** Having invested billions of dollars in in drinking water and wastewater infrastructure, the federal government has an interest in protecting its investment and ensuring that future assistance goes to utilities that are built and managed to meet key regulatory requirements. **The General Accounting Office (GAO) found that drinknig water and wastewater utilities benefited from comprehensive asset management, but also had implementation challenges.** The benefits include: improved decision making about their capital assets, and more productive relationships with governing authorities, rate payers, and others. Among challenges to implementing asset management, utilities cited collecting and managing needed data and making the cultural changes necessary to integrate information and decision making across departments. The highlights for this report can be found at http://www.gao.gov/highlights/d04461high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−461

[Return to top]

Public Health Sector

17. *April 21, ic Scotland* — **Scientists warn over bioterror. Better ways of detecting and dealing with chemical and biological agents must be found, leading United Kingdom (UK) scientists are warning.** The problem was investigated by the Royal Society after the 2001 postal anthrax attacks in the United States. The Royal Society's findings are expected to echo those from the Commons Science and Technology Committee which were rejected by the UK Government last year. Chairman Ian Gibson said ministers should now listen to advice and raise their game. Gibson said scientists should be gathered together in one center even if it was a "virtual center". This would let them "talk together and share their ideas and understanding of how to detect organisms, what organisms there might be", he said. "The Government hasn't

even got its plans correct in terms of the organisms that might be released in a terrorist attack. "There are two different tables that have been published. "So there are all sorts of little things they have to get right."
Source: http://icscotland.icnetwork.co.uk/news/uk/tm_objectid=14166186&method=full&siteid=50141&headline=scientists−warn−over−bi o−terror−name_page.html

18. *April 21, Associated Press* — **Inspectors find lax security at university labs.** Government inspectors have identified serious weaknesses in security at university laboratories that perform research on anthrax and other dangerous substances. **The 11 universities that receive taxpayer money for the research were lax in controlling access to the labs and kept poor inventories of the materials, the Health and Human Services inspector general said.** "Physical security weaknesses at all 11 universities left several agents vulnerable to theft or loss, thus elevating the risk of public exposure," said a summary report of the inspections, conducted in 2002 and 2003. The report said the universities have started correcting the problems, which the inspector general has not verified.The universities selected were those that received grants from the National Institutes of Health for research on "select agents," 42 pathogens and toxins that pose the greatest dangers to the public's health. **At all 11 universities, the report said, once inside the buildings, "intruders had unobstructed access to the floors" with the critical labs. Keys to those labs were too widely available, security doors and freezers in the labs were left unlocked, closed−circuit television cameras were not used, and ID badges were not required, the report said.** The report is available at http://oig.hhs.gov/oas/reports/region4/40402000.pdf
Source: http://www.signonsandiego.com/news/nation/20040420−1522−anth rax−labs.html

19. *April 21, Washington Post* — **Infection leads to quarantine at pet store. Twenty−five birds at a Petco store in Fairfax City, VA, have been quarantined after one parakeet was found to have a communicable infection that can be passed to humans and result in flu−like symptoms and sometimes pneumonia, according to officials with the Virginia Department of Agriculture and Consumer Services.** Officials said the diagnosis was made last week of psittacosis, a respiratory infection also known as "parrot fever" that can be transmitted to humans who inhale the dried secretions of an infected bird. Bird owners, pet shop employees, and veterinarians generally run the highest risk of contracting the illness. State officials said the risk to customers who have visited the store is minimal. Petco employees have been briefed on the health risks and will be watching for symptoms, health officials said.
Source: http://www.washingtonpost.com/wp−dyn/articles/A29342−2004Apr 20.html

20. *April 21, New York Times* — **Security system at hospitals draws scrutiny. New York City's 11 public hospitals have no common security system, no uniform method of screening visitors or restricting their access to certain wards of a hospital building.** Background checks on new employees can vary widely from one institution to another. **In fact, despite the employment of its own 850−member police force, the municipal hospitals have put in place relatively few systemwide security measures.** Hospital officials say the hospitals and the more than 100 community clinics, diagnostic centers, and nursing homes in the system share security concerns every other month, at meetings of the major facilities' security directors. But the officials acknowledge that the system leaves to each institution the decision on how and whether to disclose its problems. Public hospitals in New York City are already like small cities. Roughly 100,000 patients come through their doors each week for outpatient procedures,

and 20,000 more visit their emergency rooms, often in the company of family members or friends. The system employs some 35,000 people. About 5,500 patients occupy hospital beds throughout the system each day, with thousands more people coming to visit those patients.
Source: http://www.nytimes.com/2004/04/21/nyregion/21hospital.html

[Return to top]

Government Sector

21. *April 21, Federal Computer Week* — **Department of Homeland Security debuts info portal.** First responders and other federal, state and local homeland security officials can now share and access information about lessons learned and best practices through a new Web−based portal launched today, April 21. The Lessons Learned Information Sharing system found at https://www.llis.dhs.gov/ was unveiled in Oklahoma City on the ninth anniversary of the 1995 terrorist bombing that killed 168 people. The portal, which took about 18 months to develop, will allow authorized emergency and homeland security officials to share validated expertise on effective planning, training and operational practices. It also will serve as an information clearinghouse for homeland security documents, including an extensive catalog of redacted after−action reports from exercises and actual incidents, and a directory of responders and homeland security officials with particular expertise. **The portal is free to verified emergency response providers −− including law enforcement, fire, emergency medical service, emergency management, public health and homeland security officials −− and meets Department of Homeland Security standards for storing sensitive but unclassified information.**
Source: http://www.fcw.com/geb/articles/2004/0419/web−dhs−04−19−04.a sp

[Return to top]

Emergency Services Sector

22. *April 20, Reuters* — **Live, digital video heading to U.S. police cars.** Tyler, TX, next month will start to install a digital video system designed to beam TV images of any police action in real−time from the police department's 60 cruisers over a wireless network back to headquarters, Tyler police said Tuesday, April 20. **They said this will be the first digital video network for cruisers in a U.S. police force. Numerous police forces currently use dashboard−mounted video cameras that record police stops on tape.** The cars will eventually be linked through a wireless network so that headquarters can see events unfold live. The computer record from the police car will be downloaded each day and placed into computer storage. Data from the car, such as readings on a radar gun, will be matched with the digital video, along with information from the magnetic strip of a driver's license that is swiped by police. **The system allows for quick retrieval of the video and data of a police stop, which can be used as evidence in court or by a citizen charging the police with unlawful conduct.** The system cost about $6,000 to $7,000 per vehicle for a basic package and about $10,000 to $12,000 for a top of the line network that also offers a huge amount of storage for the computers back at police headquarters.
Source: http://www.cnn.com/2004/TECH/ptech/04/20/police.videos.reut/ index.html

[Return to top]

Information and Telecommunications Sector

23. *April 20, US−CERT* — **Technical Cyber Security Alert TA04−111B: Cisco IOS SNMP Message Handling Vulnerability.** There is a vulnerability in Cisco's Internetwork Operating System (IOS) SNMP service. When vulnerable Cisco routers or switches process specific SNMP requests, the system may reboot. **If repeatedly exploited, this vulnerability could result in a sustained denial of service (DoS)**. Cisco has published detailed information about upgrading affected Cisco IOS software to correct this vulnerability. System managers are encouraged to upgrade to one of the non−vulnerable releases. Additional information is available on the Cisco Website:
http://www.cisco.com/warp/public/707/cisco−sa−20040420−snmp. shtml
Source: http://www.us−cert.gov/cas/techalerts/TA04−111B.html

24. *April 20, The Register* — **NetSky−X circulating in Europe.** NetSky−X, the latest in an ever−expanding series of computer worms, displays a dalliance with foreign languages previously unknown among virus writers. The latest Windows−only nuisance sends messages in either English, Swedish, Finnish, Polish, Norwegian, Portuguese, Italian, French or German. **The "polyglot worm" is spreading extensively, particularly in mainland Europe. This spread is doubtless helped by the fact most users will be thrown by seeing an infectious email in their own language and not English, as is the norm**. That's not to say the unknown author of the worm is any good at languages, though. "In many cases the messages are composed incorrectly suggesting that the worm's author did not ask native speakers for translation or used an on−line translation service like Babel Fish," Finnish AV firm F−Secure notes. The worm contains a payload which attempts to launch a DoS (Denial of Service) attack on three German language Websites between April 28 and 30.
Source: http://www.theregister.co.uk/2004/04/20/babel_fish_worm/

25. *April 20, ZDNet (UK)* — **New hacking tool: chocolate.** A survey of 172 office workers in London found that almost three quarters would reveal their network−access password in exchange for a bar of chocolate. The survey was conducted by the organizers of Infosecurity Europe 2004, a security exhibition to be held in London next week. Claire Sellick, event director for Infosecurity Europe 2004, said the results prove that employers are not educating their users about the importance of information security: "This comes down to poor training and procedures. Employers should make sure that their employees are aware of information security policies and that they are kept up−to−date," she said. **According to the survey, most participants were unhappy remembering so many different passwords and would prefer to use either biometric authentication−−such as fingerprint recognition−−or smartcards**. At the RSA Security conference in San Francisco last month, Microsoft's chairman **Bill Gates said traditional passwords are dying out because they cannot be relied on to keep critical information secure**.
Source: http://zdnet.com.com/2100−1105_2−5195282.html

26. *April 20, eSecurity Planet* — **Exploit for Windows SSL flaw circulating.** A week after Microsoft announced a SSL vulnerability affecting key Windows products, malicious hackers

unveiled exploits that could lead to widespread denial−of−service attacks. **The exploit code, described in the underground as the "SSL Bomb," could allow specially crafted SSL packets to force the Windows 2000 and Windows XP operating systems to block SSL connections. On Windows Server 2003 machines, the code could cause the system to reboot**. Microsoft issued a patch in its MS04−001 advisory but according to the SANS Institute it's only a matter of time before exploits with remote code execution appear in the wild. SANS also warned of a variant of the Gaobot.XZ worm which has been actively scanning ports to try to explore an old vulnerability of the UPnP service, described in Microsoft Security Bulletin MS01−059. The worm targets multiple vulnerabilities to spread, including the DCOM RPC vulnerability (Microsoft Security Bulletin MS03−026); the WebDav vulnerability (Microsoft Security Bulletin MS03−007); and the Workstation service buffer overrun vulnerability (Microsoft Security Bulletin MS03−049).
Source: http://www.esecurityplanet.com/prodser/article.php/3343011

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_NETSKY.P** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 80 (www), 445 (microsoft−ds), 3127 (mydoom), 2745 (urbisnet), 137 (netbios−ns), 1434 (ms−sql−m), 1025 (blackjack), 6129 (dameware), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *April 21, New York Times* — **Sweden arrests four men it links to terrorism.** The police in Sweden arrested four men on Tuesday, April 20, in connection with what officials called Islamic terrorism. The Swedish newspaper Aftonbladet reported that the suspects had been seized at the urging of United States authorities because they had helped organize attacks on American forces in Iraq. **Swedish television said later that the suspects were between 25 and 35 years old and residents of Sweden. It identified two of those arrested as Iraqi citizens and said a third was born in Jerusalem and had American citizenship**. The 35−year−old suspect was said to have been born in Lebanon but had become a Swedish citizen. There was no official confirmation of that report.

Source: http://www.nytimes.com/2004/04/21/international/europe/21swed.html?adxnnl=1&adxnnlx=1082561450−1i3UPKSi7ojR/d2gUA+Zkw

28. *April 21, The Christian Science Monitor* — **Saudi bomb: a shift in al Qaeda tactics.** Suspected al Qaeda militants struck their first major Saudi target Wednesday, April 21, when a suicide car bomber blew himself up in front of national police security headquarters. **The attack is seen by Saudi analysts as a tactical shift in a growing confrontation here between Islamist militants linked to al Qaeda and the Saudi government.** The attack in Riyadh comes within days of a major crackdown on militants which netted eight suspects, weapons caches, and five booby−trapped cars laden with more than four tons of explosives. **Last month, a militant group linked to al Qaeda vowed to avenge the killing of a leading al Qaeda figure in Saudi Arabia and said it would start targeting Saudi security forces if they continued to hunt down Muslim fighters.** The blast, which shattered the entire glass front of the General Security building, destroyed cars as far as several hundred yards away. The Associated Press reported nine dead, but at this time there is no official report the number of deaths.
Source: http://www.csmonitor.com/2004/0422/p05s01−wome.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at info@us−cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.